3.2 weakness of expanded key

The MISTY1's compact schedule contributes to high implementing performance. However, there are very simple relations among expanded-keys produced by the key schedule. Therefore, number of particular plaintexts and complexity for decryption attack becomes smaller to perform multiple-step decryption attack.

If the extended key used by the AND operation contains only zeros and the extended key used by the OR operation contains only ones, the output of the FL function is the exclusive-or of its input and a constant. Thus, if we fix the extended keys as follows,

$$KL_{21} = KL_{31} = 0x0000$$
$$KL_{22} = KL_{32} = 0xffff \qquad (9)$$

With this assumption, it is known that value of seventh order difference of MISTY at the third round becomes a constant by references [1][3][5][11][13], and this condition is calculated back from the key schedule to be the key condition relation to the user key. Thus

$$K_3^{'} = K_2 = 0x0000$$

$$K_5 = K_8^{'} = 0xffff \qquad (10)$$

where

$$K_3^{'} = KI(K_3;K_4)$$

$$K_3^{'} = KI(K_3;K_4) \qquad (11)$$

Consequently, decryption attacker need to fix the secret key sub-blocks , K_1, K_2, K_3, K_4, K_5 and K_8 .

However, we can show that the number of fixed secret key sub-blocks becomes small if we use an eighth order differential for the attack. In the case of fixed KL_3, reference [13] shows the degree of the left-most 7 bits in the output of KO_3 ($Z_3^{'L_7}$) is 9.

However, the degree of the left-most 7 bits is 7 analytically, thus.

$$\Delta^{(7)} Z_3^{'L_7} = 0x6d$$

In the case of NOT fixed KL_3, the formal degree of output of FI_{31} and FI_{32} is estimated 9, and the formal degree of $Z_3^{'L_7}$ is estimated to be 8.

Comparing these estimations, we conjecture that the degree of $Z_3^{'L_7}$ for NOT fixed KL_3 is 7 but decryption attacker can not specify the value of its seventh order differential (see fig 4).

From the value of higher order differentials, it is easy to see that if $\Delta^{(N)}Z$ is constant, then $\Delta^{(N+1)}Z$ is equal to 0. Since the attacker cannot specify the value of the seventh order differential of $Z_3^{'L_7}$, we consider an attack using the eighth order differential.

Moreover, we consider the case of NOT fixed KL_{21}. Half left bits of the plaintext and sub-blocks X_2 and X_3 affect the maximum degree of output. Therefore we cannot use them as variable bits. Thus we consider an eighth order differential using X_0 and one bit selected from among X_1. We confirmed that $\Delta^{(8)}Z_3^{'L_7} = 0$ for such an eighth order differential by computer simulation.

The attack equation derived from the equation $\Delta^{(8)}Z_3^{'L_7} = 0$ has unknowns with respect to expanded keys for FL_6 and FO_5. However, if we fix the value of the secret key sub-block as $K_7 = KL_{62} = 0xffff$, we have $\Delta^{(8)}Z_3^{'L_7} = 0$. We can neglect the unknowns with respect to the expanded keys for FL_6.

Our attack succeeds under the condition that the secret key sub-blocks satisfy $K_5 = K_7 = 0xffff$

Therefore it is possible to attack by using eighth order differential at third round.

SCIS 2003 The 2003 Symposium on Cryptography and Information Security
Hamamatsu,Japan, Jan.26-29,2003
The Institute of Electronics,
Information and Communication Engineers

鍵スケジュールを考慮したブロック暗号に対する攻撃に関する一考察

A study on attack considering key schedule against block ciphers

田中秀磨* Hidema Tanaka　　杉尾信行† Nobuyuki Sugio　　金子敏信† Toshinobu kaneko

あらまし 本論文では鍵スケジュールを考慮したブロック暗号に対する攻撃について述べる。攻撃者は都合の良い拡大鍵の条件について探索し、鍵スケジュールを用いて秘密鍵の条件を導出する。条件付き秘密鍵のもとで、拡大鍵同士の関係を利用して攻撃方程式を解くコストを減少させ、攻撃適用可能範囲を拡大させる。秘密鍵に条件を付けることから、本攻撃手法は、弱鍵を利用した攻撃方法の一つである。本攻撃の有効性について6段MISTY1に対する攻撃で確認した。MISTY1は8段で構成されるが、128[bit]秘密鍵のうち32[bit]に条件をつけ、6段まで段数を減少させた場合、8階差分を用いた攻撃が可能であることが分かった。本攻撃には$2^{18.9}$個の選択平文と$2^{80.9}$の計算量が必要である。

キーワード ブロック暗号、鍵スケジュール、MISTY1、高階差分攻撃

1 はじめに

ブロック暗号に対する攻撃方法は数多く提案されているが、その大部分は暗号化関数に主眼が置かれ、鍵スケジュールを考慮することはまれである。本論文では鍵スケジュールにも着目し、既存の攻撃方法と組み合わせることにより、さらに効果的な攻撃が行えることがある場合を示す。攻撃者は都合の良い拡大鍵の条件について探索し、鍵スケジュールを用いて秘密鍵の条件を導出する。条件付き秘密鍵のもとで、拡大鍵同士の関係を利用して攻撃方程式を解くコストを減少させ、攻撃適用可能範囲を拡大させる。このような手順で攻撃を行い秘密鍵に条件を付けることから、本攻撃手法は弱鍵を利用した攻撃方法の一つであるが、さらにその条件を他の拡大鍵にも波及させることが、本方式の特徴である。このため、通常の攻撃方法では最終段の拡大鍵を解くための方程式を導出するが、本方式では、直接秘密鍵を求める方程式を導出できることも示す。本方式は、汎用なブロック暗号に対する攻撃方法と組み合わせることが可能であるが、本論文では高階差分攻撃との組み合わせについて述べる。また、攻撃方程式を解く方法として代数的解法を用いた。鍵スケジュールを考慮した攻撃の場合、通常の攻撃に比べて未知数が少ないので、2段消去型攻撃が効果的になると考えられる。そのため、全数探索と代数的解法を組み合わせた攻撃方程式の解く場合に必要となる、選択平文数と計算量の見積もりについても示した。

さらに、攻撃の具体的な例としてMISTY1[8]に対する攻撃を示す。MISTY1はNESSIE[16]やCRYPTREC[17]で標準暗号の候補となっている、64bitブロック暗号であり、その実装性能は同一カテゴリ中最良と目されている。また、提案されてから5年以上となり多数の攻撃論文も発表されている。本論文で示す結果は、6段MISTYの場合、8階差分を用いた攻撃が可能であり$2^{18.9}$個の選択平文と$2^{80.9}$の計算量が必要なことを示している。本結果は、MISTYに対するものの中で最高の結果である。

2 準備

2.1 鍵スケジュールと拡大鍵

通常、ブロック暗号はユーザが決定した秘密鍵を鍵拡大関数に入力し、各段で使用する拡大鍵を生成する。これは、同一の鍵を各段で使用するよりも出力のランダム性が増すと予測されることと、一部の拡大鍵が攻撃者に破られたとしても、もとの秘密鍵に辿り着くのを困難にする目的があると考えられる。

拡大鍵を生成する方法には様々なものがある。例えば、暗号化関数と全く別の関数を用意する場合である。この場合、拡大鍵と秘密鍵の関係は平文と暗号文の関係と全く異なるので上述の出力のランダム性に貢献すると考えられる。しかしながら、実装においては2種類の関数を用意する必要が生じるなどの欠点もある。実装性を重視するならば、暗号化関数の一部を鍵拡大関数として利用す

* 独立行政法人通信総合研究所情報通信部門非常時通信グループ〒184-8795 東京都小金井市貫井北町 4-2-1, Emergency Communications Group, Communications Research Laboratory 4-2-1 Nukui-Kitamachi, koganei, Tokyo 184-8795
† 東京理科大学理工学部電気工学科〒278-8510 千葉県野田市山崎2641, Department of Electrical Engineering Faculty of Science and Technology, Tokyo University of Science 2641 Yamazaki, Noda, Chiba 278-8510

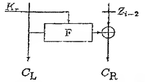

図 1: i 段の F 関数で構成された場合の最終段

る方法や、テーブル参照する方法が揚げられる。この場合、前述のような実装性における欠点を克服することができるものの、秘密鍵と拡大鍵の関係が単純になり易いので弱鍵などの問題点も生じやすくなると考えられる。

鍵拡大関数は、直接に暗号それ自体の安全性を脅かすものとはなり得ないものの、その設計があまりにも単純な場合、拡大鍵から秘密鍵を容易に求めることを攻撃者に許す場合があることを示すことが本論文の目的である。このような視点に立てば、ブロック暗号に対して既に適用されている様々な攻撃方法と組み合わせて論じることができるが、本論文では高階差分攻撃に限定する。

2.2 高階差分 [7]

$X \in \mathrm{GF}(2)^n$ を変数ベクトルとする。

$$X = (x_1, x_2, \ldots, x_i), \qquad x_i (i = 1, 2, \ldots, n) \in \mathrm{GF}(2)^n$$

$F(\cdot)$ を鍵 K を含む暗号化ブール関数とする。また、$Y \in \mathrm{GF}(2)^m$ を出力とする。

$$Y = F(X; K) \tag{1}$$

$(A_1, A_2, \ldots, A_i)$ を $\mathrm{GF}(2)^n$ 上で 1 次独立な i 個のベクトルとする。これらによって張られる、$\mathrm{GF}(2)^i$ の部分空間を $V^{(i)}$ で表わす。関数 $F(X;K)$ の X に関する i 階差分 $\Delta^{(i)}_{V^{(i)}} F(X;K)$ は以下の式で定義される。

$$\Delta^{(i)}_{V^{(i)}} F(X;K) = \bigoplus_{A \in V^{(i)}} F(X \oplus A; K) \tag{2}$$

以下、特にこだわらない限り $\Delta^{(i)}_{V^{(i)}}$ を $\Delta^{(i)}$ と略記する。関数 $F(X;K)$ の X に関する次数が N であるならば、X, K に依存せず、

$$\deg_X\{F(X;K)\} = N \Rightarrow \begin{cases} \Delta^{(N+1)} F(X;K) = 0 \\ \Delta^{(N)} F(X;K) = \text{const} \end{cases} \tag{3}$$

が必ず成立する。

2.3 攻撃方程式

i 段で構成された Feistel 型暗号の場合、F 関数出力側の $i-2$ 段目の出力値 Z_{i-2} は、i 段目の出力と排他的論理和され暗号として出力される (図 1)。入力 X に対する $i-2$ 段目の出力次数が N であれば、Z_{i-2} の高階差分値は式 (3) より

$$\begin{cases} \Delta^{(N+1)} Z_{i-2}(X) = 0 \\ \Delta^{(N)} Z_{i-2}(X) = \text{const} \end{cases} \tag{4}$$

が成立する。一方、最終段である i 段目において

$$F(C_{\mathrm{L}}(X); K_i) \oplus C_{\mathrm{R}}(X) = Z_{i-2}(X) \tag{5}$$

という関係が成り立つ。K_i は最終段で使用される鍵であり、$C_{\mathrm{L}}(X), C_{\mathrm{R}}(X)$ は平文 X に対応する暗号文の左ブロックと、右ブロックである。式 (4) と式 (5) より、以下が成立する。

$$\begin{cases} \bigoplus_{A \in V^{(N)}} F(C_{\mathrm{L}}(X); K_i) \oplus C_{\mathrm{R}}(X) = \text{const} \\ \bigoplus_{A \in V^{(N+1)}} F(C_{\mathrm{L}}(X); K_i) \oplus C_{\mathrm{R}}(X) = 0 \end{cases} \tag{6}$$

式 (6) は、未知である鍵 K_i が正しい時、等号が成立する。従って、式 (6) を解くことにより真の鍵 K_i が得られるので、以下これを攻撃方程式と呼ぶ。

2.4 代数的解法

b bit の出力 sub-block に注目して N 階差分を用いて攻撃方程式を導いたとして、それを解くのに必要な選択平文数と計算量について見積もる。本論文では、下山、盛合、金子によって提案された代数的解法の適用を考える [9][10]。代数的解法は、未知数による高次項を新たな未知数と再定義することにより、もともとは高次の方程式であった攻撃方程式を線形方程式へ変形し、解くための計算量を大幅に引き下げるものである。

攻撃方程式を線形方程式へ変形した後の再定義された未知数の合計を L とする。代数的解法は $L \times L$ の係数行列を計算し、その後、Gauss-Jordan 消去法などを用いて方程式を解く。今、b bit の sub-block に注目して攻撃方程式を導出しているので、一つの N 階差分から b 個の線形方程式が得られることになる。全ての未知数を決定するために $\lfloor L/b \rfloor$ の N 階差分が必要となる。文献 [9][10] と同じ方法で係数行列を計算するには $2^N \times \lfloor L/b \rfloor \times L$ 回の F 関数計算が必要となる。

ここで、さらに別の s bit の未知数 S を全数探索で見積もりながら、攻撃方程式を解くのに必要な選択平文数と計算量について見積もる。もし、さらに α 個余分な方程式を用意すれば、$2^{-\alpha}$ の確率で偽の S が成立することになる。それ故、もし $2^{s-\alpha} << 1$ を満たす α があれば、偽の S は全て排除することができる。従って、全数探索と代数的解法を組み合わせた方法で攻撃方程式を解くためには、$2^N \times \lfloor (L+\alpha)/b \rfloor$ の選択平文と $2^{N+\alpha} \times \lfloor (L+\alpha)/b \rfloor \times L$ 回の F 関数計算が必要となる。以下では F 関数計算の回数を単に計算量と呼ぶ。

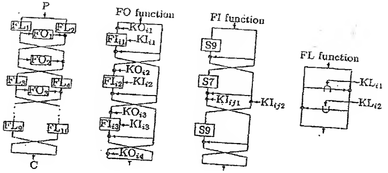

図 2: MISTY1

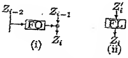

図 3: Variables

3 具体的な攻撃例

3.1 MISTY1

MISTY は、三菱電機の松井によって 1996 年に提案された 64 ビットブロック暗号である [8]。構造は Feistel 型であり、8 段で構成される (図 2)。FO 関数と呼ばれるラウンド関数が、FI 関数と呼ばれる内部関数による Feistel 構造を構成する入れ子型になっている特徴がある。さらに FI 関数内は 7bit と 9bit の非対称 Feistel 型構造である。MISTY は、FL 関数という付加関数を持つが、これの無い FO 関数のみの 3 段構成で、線形攻撃と差分攻撃に対し証明可能安全性を持つ。FL 関数は、この証明可能安全性を崩さないように設計され、他の攻撃に対する安全性確保を期待されている。

MISTY の安全性については、既に様々な結果が報告されている。MISTY は上述のように、安全性の大部分が FO 関数で実現されているので、FL 関数の無い場合についての評価結果も数多くあるが、ここでは FL 関数を省略しないものについて考える。現在、最も成功している攻撃結果は Knudsen と Wagner による Integral Attack[3]、楽野による高階差分攻撃 [15] によるものであり、両者とも 5 段構成の場合が攻撃可能であることを示している[1]。また、Kühn[5][6] も不能差分による攻撃結果を示している。

本論文で使用する表記について説明する。平文 P は以下のように分割できる。

$$
\begin{aligned}
P &= (P_L \| P_R) \\
&= (X_{15}, \ldots, X_8 \| X_7, \ldots, X_0) \\
X_i &\in \begin{cases} GF(2)^7 : i = \text{even} \\ GF(2)^9 : i = \text{odd} \end{cases}
\end{aligned}
\tag{7}
$$

MISTY1 は 2 種類の S-Box、$S7$ と $S9$ を FI 関数中で用いる。$S7$ の代数次数は 3 であり、$S9$ の代数次数は 2 である。表 1 に鍵スケジュールを示す。

$$
\begin{aligned}
K &= (K_7, \ldots, K_0), \quad K_i \in GF(2)^{16} \\
K'_i &= FI(K_i; K_{i+1})
\end{aligned}
\tag{8}
$$

また、図 3 に示すように中間変数 Z_i と Z'_i を用いる。これらは FL 関数が FO 関数の後に存在するか否かで使用する方法が変わる。つまり、FL 関数が FO 関数の後に存在する場合、FO 関数からの出力は Z'_i と書き換えられ、その後の FL 関数からの出力を Z_i とする。それ故、$Z'_{-1} = P_L$ と $Z'_0 = P_R$ となる。さらに、sub-blockQ_i の左端 $m$bit に注目する時は $Q_i^{L_m}$ と表記する。また、Q_i の N 階差分は $\Delta^{(N)} Q_i$ と略記する。

3.2 攻撃に都合の良い拡大鍵

MISTY1 はコンパクトな鍵スケジュールを持ち、実装性において大いなるアドバンテージとなっている。しかしながら単純な構造であるため、拡大鍵間の関係が非常にシンプルである。それ故、攻撃を行うにあたり必要な選択平文数/計算量を少なめに抑えながら、多段の攻撃が可能となる可能性がある。

[1] Knudsen と Wagner の攻撃モデルは最終段に FL が存在しない。一方、楽野の攻撃モデルは最終段に FL が存在する。両者とも 5 段構成を攻撃しているが、どちらが有効かを論じるのは本論文の中心ではないので避ける。しかしながら設計者が想定していない段数についての攻撃結果とはいえ、賛否の分かれるところではあるが、攻撃者の美意識としては楽野モデルが適当と思われる。

表 1: MISTY1 の鍵スケジュール

Sub-key	KO_{i1}	KO_{i2}	KO_{i3}	KO_{i4}	KI_{i1}	KI_{i2}	KI_{i3}	KL_{i1}	KL_{i2}
Secret key sub-block	K_i	K_{i+2}	K_{i+7}	K_{i+4}	K'_{i+5}	K'_{i+1}	K'_{i+3}	K_i (odd i) K'_{i+1} (even i)	K'_{i+6} (odd i) K_{i+3} (even i)

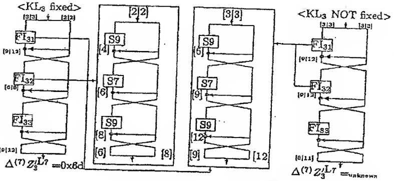

図 4: FO_3 に関する形式的な代数次数

もし、FL 関数内において AND 演算で使用される拡大鍵の値が all-zero、OR 演算で使用される拡大鍵が all-one であるならば、FL 関数の出力はその入力に定数を排他的論理和しただけとなる。それ故、以下のように拡大鍵を固定した場合について考える。

$$KL_{21} = KL_{31} = 0x0000$$
$$KL_{22} = KL_{32} = 0xffff \qquad (9)$$

すると、既にいくつかの文献 [1],[3],[5],[11],[13] などで示されているように、3 段目の出力の 7 階差分値は定数となる。鍵スケジュールから、この条件を逆算すると、鍵 sub-block は以下のように固定されたことになる。

$$K'_3 = K_2 = 0x0000$$
$$K_5 = K'_8 = 0xffff \qquad (10)$$

ただし

$$K'_3 = FI(K_3; K_4)$$
$$K'_8 = FI(K_8; K_1) \qquad (11)$$

結果として、7 階差分を用いて 3 段目出力に注目して攻撃方程式を導出する場合、攻撃者は $K_1, K_2, K_3, K_4, K_5, K_8$ を固定しなければならない。

しかしながら、もし 8 階差分を用いた攻撃ならば、固定しなければならない鍵 sub-block の数を少なくすることができることを示す。KL_3 を固定した場合、FO_3 からの出力の左 7bit($Z_3^{\prime L7}$) の形式的代数次数が 9 次となることが文献 [13] で示されている。しかしながら、解析的には 7 次であり $\Delta^{(7)} Z_3^{\prime L7}$ =0x6d となる。KL_3 を固定しない場合、FI_{31} と FI_{32} の出力の形式的代数次数が 9 次となり、その排他的論理和である $Z_3^{\prime L7}$ の代数次数は 8 次となる。これらの見積もりを比較すると、KL_3 を固定しない場合の出力の代数次数も 7 次であるが、その 7 階差分値は攻撃者に予測できないと予想できる (図 4 参照)。

高階差分の性質から、$\Delta^{(N)} Z$ が定数であれば $\Delta^{(N+1)} Z$ は 0 である。$Z_3^{\prime L7}$ の 7 階差分値を攻撃者は特定することができないので、8 階差分を用いた攻撃について考える。さらに、KL_{21} を固定しないことも考える。平文の左半分と X_2 と X_3 は、直接的に出力の代数次数を上昇させるので、ここから新たな変数 bit を選ぶことはできない。従って、X_0 の 7bit と X_1 から選んだ 1bit の合計 8bit による 8 階差分について考えた。計算機実験の結果、$\Delta^{(8)} Z_3^{\prime L7}$ =0 となることが確認できた。

$\Delta^{(8)} Z_3^{\prime L7}$ = 0 の事実を用いて攻撃方程式を導くと、FL_6 と FO_5 で使用される鍵に関する方程式となる。しかしながら FL_6 での鍵も解くとなると、攻撃方程式が複雑になり、解くためのコストの増加を招くので、ここでは $K_7 = KL_{62}$=0xffff と固定し、FL_6 の出力に対する 8 階差分、$\Delta^{(8)} Z_3^{\prime L7} = 0$ を用いて攻撃を行う。

この結果、もし秘密鍵の sub-block が $K_5 = K_7$ =0xffff を満たすならば、3 段目出力に対する 8 階差分値を用いた攻撃が可能となることが分かった。

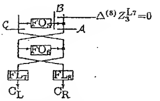

図 5: 攻撃方程式の中間変数の関係 $\mathcal{A}$, $\mathcal{B}$ and $\mathcal{C}$

3.3 8階差分を用いた攻撃

一般的には、攻撃者は最終段で使用される拡大鍵に対して攻撃方程式を導出してそれを定め、決定した鍵を使ってさらに上の段の拡大鍵を求める、という手順を踏む。本論文では、直接に秘密鍵 sub-block を求めるので、最終段への攻撃がそのまま秘密鍵の決定につながる。これは、拡大鍵と秘密鍵の関係を決定している鍵スケジュールが単純なためである。

秘密鍵 sub-block が S-Box に入力される回数が多くなると、秘密鍵に関する次数が高くなり、独立な未知数の数が爆発的に増加するので攻撃方程式を解くのが困難になる。それ故、S-Box への入力回数をなるべく少なくし、攻撃方程式中の未知数の代数次数を低く抑えることが必要となる。このような考え方のもとで、2段消去型攻撃 [12] を想定し、どの未知数を全数探索で定め、どれを代数的解法で定めるか、効果的な組み合わせについて考える。

攻撃方程式は以下のように導ける[2]。

$$\Delta^{(8)} Z_3^{L7} = \Delta^{(8)}\{\mathcal{A}+\mathcal{B}\} = 0,$$

$$\left\{\begin{aligned}
\mathcal{A} &= \mathrm{FL}_8(\mathrm{C_R};\mathrm{KL}_8)^{\mathrm{L7}}\\
&= \mathrm{FL}_8(\mathrm{C_R};K_5',K_8)^{\mathrm{L7}}\\
\\
\mathcal{B} &= \mathrm{FO}_5(\mathcal{C};\mathrm{KO}_5,\mathrm{KI}_5)^{\mathrm{L7}}\\
&= \mathrm{FO}_5(\mathcal{C};K_1,K_2',K_4,K_5,K_6',K_7,K_5')^{\mathrm{L7}}\\
\\
\mathcal{C} &= \mathrm{FL}_7(\mathrm{C_L};\mathrm{KL}_7)\\
&\quad +\mathrm{FO}_5(\mathrm{FL}_8(\mathrm{C_R};K_5',K_8);\mathrm{KO}_6,\mathrm{KI}_6)\\
&= \mathrm{FL}_7(\mathrm{C_L};K_2',K_4)\\
&\quad +\mathrm{FO}_6(\mathrm{FL}_8(\mathrm{C_R};K_6',K_8)\\
&\qquad ;K_1',K_2,K_3',K_5,K_7',K_8)
\end{aligned}\right. \tag{12}$$

攻撃方程式中の中間変数 $\mathcal{A},\mathcal{B},\mathcal{C}$ は図 5 である。

K_5 と K_7 は既に固定されているので、合計 96bit の 6 つの秘密鍵 sub-block を解くことを考える。KO_{61}, KO_{62},KI_{61} は、S-Box に入力される回数が最大となるので、前述のように代数的解法で定めるのは困難である。それ故、$K_6(=\mathrm{KO}_{61})$, $K_8(=\mathrm{KO}_{62})$,$K_3'(=\mathrm{KI}_{61})$ は全数探索で定めることにする。また $K_7'(=\mathrm{FI}(K_7;K_8))$ であるから、$\mathrm{KI}_{62}=K_7'$ は既知として扱うことができる。以上をまとめると以下のようになる。

$$\begin{aligned}
&K_5, K_7 = 固定,\\
&K_3', K_6, K_8 = 全数探索,\\
&K_7' = 計算可能
\end{aligned}$$

それ故、K_1,K_1',K_2,K_2' ,K_4 が代数的解法で解を定める対象の未知数である。ところで、$K_1=\mathrm{KO}_{54}$ は、定数加算として存在する。攻撃方程式は高階差分で計算されるので、K_1 に関する項は存在しない。従って、K_1', K_2, K_2', K_4 (合計 64 bit) が代数的解法で定まる。

その結果、K_1', K_2, K_2', K_3', K_4, K_5, K_6, K_7, K_8 が定まる。$K_1'=\mathrm{FI}(K_1;K_2)$ であり、$K_3'=\mathrm{FI}(K_3;K_4)$, であるから、$K_1$ と K_3 はそれぞれ (K_1', K_2) または (K_3', K_4) を用いて定めることができる。

3.4 必要な選択平文数と計算量

計算機実験により、攻撃方程式に存在する独立な未知数の数を計算した。その結果、$L=13,269$ であることが分かった。$s=48$ bit の未知数に関しては全数探索で定めるので、 $\alpha=64$ $(2^{48-64}=2^{-16} << 1)$ と設定するのが適当であろう。また、7bit の出力 sub-block Z_3^{L7} に注目しているので、$b=7$ である。従って、$2^8\times\lfloor(13269+64)/7\rfloor\simeq 2^{18.9}$ 個の選択平文と $2^{8+48}\times\lfloor(13269+64)/7\rfloor\times 13269\simeq 2^{80.6}$ の計算量があれば、攻撃方程式を解くことができる。

4 まとめ

本論文では、鍵スケジュールを考慮したブロック暗号に対する攻撃について考え、その一例として MISTY1 に対する攻撃を示した。鍵スケジュールを考慮することにより、従来型の、各段で使用される拡大鍵について求め、その後それを利用して全ての拡大鍵を求めるというプロセスを廃し、直接に秘密鍵を求めることができることを示した。本論文では高階差分攻撃に特化し、さらに攻撃方程式を解くアルゴリズムである代数的解法を拡張し、2段消去型攻撃に発展させた場合についても述べた。特に、全数探索と代数的解法を組み合わせて使用する場合、α 個余分に方程式を用意すれば良いことを示し、具体的な攻撃例では必要な選択平文数と計算量をそれほど増加させずに効果的に使用できている。また、通常は各段について未知数を独立に扱わねばならないが、鍵スケジュールを考慮することにより、その拡大鍵間の関係を用いることができるので、未知数の増加を抑えることができた。

[2] 特に理由について詳述しないが、本論文では最終段に FL 関数があることは暗黙のうちの了解事項である。

本論文で示した、MISTY1への攻撃結果は、現時点で知られている限り最高のものである。秘密鍵sub-blockに条件を付けているので、弱鍵を利用した攻撃の範疇で扱われる結果ではあるが、鍵スケジュールを考慮することによってその条件を最大限利用した。MISTY1とその派生型のKASUMIは、実装性能の面でこのカテゴリの暗号アルゴリズムの中では図抜けた性能を持っているが、若干、鍵スケジュールが単純な傾向にある。本論文での結果は、弱鍵を利用し攻撃者により優位な条件を与えている上、段数をもともとの仕様よりも少なくしているので、現実的脅威に直接繋がるものではないと考えるが、鍵スケジュールに関して、少しの改良で本論文で示した結果を覆すような仕様に変更は可能と信じる。

本論文では、高階差分攻撃と組み合わせた鍵スケジュールを利用した攻撃を示したが、特に攻撃アルゴリズムに限定された考え方ではないので汎用性の高いものと考える。今後は、他の攻撃方法と組み合わせた結果についても報告する予定である。

参考文献

[1] S.Babbage, and L.Frisch,"On MISTY1 Higher Order Differential Cryptanalysis," ICISC2000, LNCS.2015, Springer-Verlag, 2000.

[2] T.Iwata, and K.Kurosawa,"Probabilistic Higher Order Differential Attack and Secure Boolean Functions," The 2000 Symposium on Cryptographi and Information Security, SCIS2000-A-46, Okinawa, Japan, January, 2000.

[3] Lar R. Knudsen and D.Wagner,"Integral Cryptanalysis," Fast Software Encryption 2002, FSE2002, Lenven, Belgium, February, 2002.

[4] T.Jakobsen and Lar R. Knudsen,"The Interpolation Attack on Block Cipher," Fast Software Encryption 4-th International Workshop, LNCS.1008, Springer-Verlag, Berlin, 1996.

[5] U.Kühn,"Cryptanalysis of Reduced-Round MISTY," Eurocrypt 2001.

[6] U.Kühn,"Improved Cryptanalysi of MISTY1," Fast Software Encryption 2002, FSE2002, Lenven, Belgium, February, 2002.

[7] X.Lai,"Higher Order Derivatives and Differential Cryptanalysis," Communications and Cryptography, pp.227-233, Kluwer Academic Publishers, 1994.

[8] M.Matsui"Block Encryption Algorithm MISTY," Techical Report of IEICE, ISEC96-11(1996-07).(In Japanese)

[9] S.Moriai, T.Shimoyama, and T.Kaneko,"Higher Order Differential Attack of a CAST Cipher," Fast Software Encryption Workshop'98, FSE'98, Paris, March, 1998.

[10] T.Shimoyama, S.Moriai, T.Kaneko, and S.Tsujii, "Improving Higher Order Differential Attack and Its Application to Nyberg-Knudsen's Designed Block Cipher," IEICE Trans. Fundamentals, Vol.E82-A, No.9, pp.1971-1980, September, 1999.

[11] M.Sugita,"Higher Order Differential Attack of Block Cipher MISTY1,2," Techical Report of IEICE, ISEC98-4(1998-05).

[12] H.Tanaka and T.Kaneko,"An Attack of 6-round MISTY1 without FL functions,"Techical Report of IEICE, ISEC2002-41(2002-07).

[13] H.Tanaka, K.Hisamatsu, and T.Kaneko,"Strength of MISTY1 without FL function for Higher Order Differential Attack,", AAECC13 Lecture Note in Computer Science 1719, 1999.

[14] H.Tanaka, C.Ishii, and T.Kaneko,"On the strength of Block Cipher KASUMI and MISTY," Symposium on Cryptographi and Information Security, SCIS2001, Oiso, Japan, January, 2001.(In Japanese)

[15] 桑野、田中、金子「MISTY1の高階差分攻撃」, 暗号と情報セキュリティシンポジウムSCIS2002予稿集,pp.937-942

[16] NESSIE, "https://www.cosic.esat.kuleuven.ac.be/nessie/"

[17] CRYPTREC, "http://www.cryptrec.org/"